(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 January 2009 (08.01.2009)

PCT

(10) International Publication Number
WO 2009/003851 A2

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2008/057824

(22) International Filing Date: 19 June 2008 (19.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07012854.1 29 June 2007 (29.06.2007) EP

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FIN-02610 Espo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SCHMIDTKE, Uwe** [DE/DE]; Margarethe-Lachmund-Str. 34, 17493 Greifswald (DE).

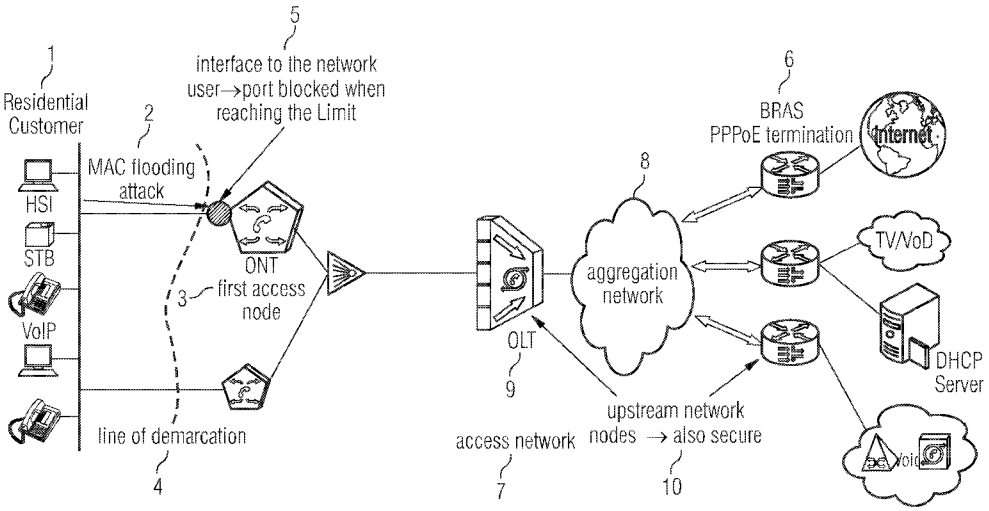
(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR / Patent Administration, 80240 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR PROTECTION A NETWORK THROUGH PORT BLOCKING



(57) Abstract: The present invention relates to a method for protecting a network against a security attack from an user, and in par ticular, for a layer 2 switch, against a MAC flooding attack. Here, the MAC flooding attack floods the layer 2 switch with at least one packet, a database is provided which saves a MAC address and its allocation and the database has a maximum quantity. The method according to the invention is character ized in that, an interface (5) between the user (1) of the network (7) and a network access functions as a line of de marcation (4). When the limit of the maximum quantity for a port (18) is reached, the port (18) is blocked during a blocking time (11). This method not just protects the first access node (3), but also the following network nodes (10) and users (1) respectively, against a security attack.

WO 2009/003851 A2

Published:

— *without international search report and to be republished upon receipt of that report*

Description

METHOD FOR PROTECTION A NETWORK THROUGH PORT BLOCKING

Technical Field

The present invention relates to a method for protecting a network, in general, against attacks from the user side (preferably Internet, networks of different providers and access networks) and in particular, for layer 2 switches against MAC flooding attacks.

Background Art

The present invention relates to a method for protecting a network against a security attack from an user, and in particular, for a layer 2 switch, against a MAC flooding attack, in which the MAC flooding attack floods the layer 2 switch with at least one packet, a database is provided which saves a MAC address and its allocation and the database has a maximum quantity, according to the preamble part of claim 1.

Such a method is known in the prior art.

MAC address is short for Media Access Control address. It is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

Layer 2 refers to the Data Link layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer is concerned with moving data across the physical links in the network.

In a network, the switch is a device that redirects data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

Nowadays, layer 2 networks, as part of the Internet or of different providers and access networks, are mainly based on Ethernet technology. The nodes of an Ethernet network are represented by worldwide unique MAC addresses.

A plurality of attacks e.g. on the Internet starts with so called „MAC flooding" attacks from the direction of the attacker. Thereby, the layer 2 network is flooded with packets which contain an excessively high number of different MAC addresses. Layer 2 switches learn MAC addresses. That is, they save the allocation "MAC address to switch port" for a certain amount of time, in order to use this information for the forwarding to the correct switch port. As long as the MAC address is unknown, a packet has to be forwarded or abolished. The database which saves the MAC addresses and their allocation, further called Forwarding Database (FDB), has a physical maximum quantity. When the limit of the maximum quantity is reached and when new addresses appear, either older addresses have to be deleted, or no additional MAC addresses will be learned

MAC flooding attacks use this effect. While flooding the network with different MAC addresses the limit of the FDB is reached. The frames towards all switch ports are flooded.

Thus, the attacker is also able to receive packets that are not addressed to him. He thereby gets information which could be used as a basis for further attacks.

In the case, when the switch deletes packets, in the case of unknown MAC addresses, Denial of Service (DoS) is reached. That is, the work of the switch is disrupted and other participants are affected.

Because of MAC flooding, software based MAC learning could lead to an overload of the CPU.

With the increasing use of the Ethernet technology in access networks as part of the provider nets the problem even expands. The user, at the boarder of the access network, must be seen as an user who needs to be protected as well as a possible attacker.

A prior art method of layer 2 switches for protecting against MAC flooding attacks, is by just allowing a limited number of MAC addresses per switch port and by not saving every further MAC address in its database (FDB), when reaching the limit in this port.

A further means are static entries. When the MAC addresses or address areas to special ports are known, they can be entered statically per configuration and the learning of these ports can be turned off.

When it's known, that in the normal case special ports do not communicate with each other, the forwarding between the ports can be basically turned off. This method is also called „port isolation".

A further often used method is the separation of the layer 2 network into so called „broadcast domains". That is, the layer 2 nets are separated into sections and just within these sections, forwarding, on the basis of the layer 2 addressing, is possible. A method is e.g. the layer 2 VLAN according to IEEE 802.1Q.)

However, the above described prior art methods, Port Isolation, VLAN Separation and limiting of the MAC addresses to be learned, protect just the node itself. The packets, which had actually already been identified as dangerous, reach further into the network and reach subsequent net nodes and net users respectively.

It is the object of the present invention to provide the aforementioned method, in such a manner that not just the access node, but also the subsequent net nodes and net users respectively are secure from security attacks in the whole network.

The solution of this invention is provided by the aforementioned method, according to the invention, according to the characterizing part of claim 1, by an interface between the user of the network and a network access, which functions as a line of demarcation. When the limit of the maximum quantity for a port is reached, the port is blocked during a blocking time.

An advantageous embodiment of the method according to the invention is the fact that the limit is specified per configuration, when an alterable limit is required. The limit can also be preferably specified per default.

Another beneficial embodiment of the method is the fact that the blocking time is greater than the aging time. This makes sense since the network nodes have deleted the former MAC addresses of the corresponding port. Thereby, an overflow can be prevented.

Preferably the aging time is 200 s. However this time can be altered. Therefore, the blocking time should not be strictly bound to the time in the first node however it should be configurable.

Another beneficial embodiment of the method is the fact the blocking time can be adjusted separately. It is thereby more flexible and independent from the aging time.

Preferably the blocking time can comply with its own MAC aging time (12). Thus, after its expiration, entries in the own FDB entries are deleted.

In order to prevent strong toggling of the port state, a hysteresis can be preferably considered between blocking and unblocking. Between a reasonable upper limit of MAC addresses per port and the number of MAC addresses, from which a MAC spoofing attack is successful, is a large range. Smaller access nodes usually own a FDB in dimensions of a few thousand entries.

An advantageous embodiment is the fact that with this method it is easy to find two different reasonable limits, for blocking and unblocking of the port.

Preferably the method according to the invention can be switched off.

Detailed Description of the Invention

The invention will be further described with reference to the accompanying drawing.

Brief Description of the Drawings

Figure 1 shows an example of an access network, according to the invention.

Detailed Description of the Drawings

Figure 1 illustrates an example of an access network (7). The access network (7) hereby is realised with the (help of) the PON technology. The first network node (3), the ONT, implements the here described method.

The interface (5) between the user (1) of the access network (7) and the network access, like e.g. the xDSL line or an Ethernet interface, can be seen as line of demarcation (4). In order to protect the access network (7) and its users, this is an effective point to stop the attacks already on the border of the access network (7).

Network access nodes (3) which provide the network accesses are for example the DSLAM or the ONT and the ONU of a PON network respectively.

The here described method describes an additional mechanism compared to the prior art. When the limit (17) for a port (18), per configuration or per default, provided limit (17) is reached, this port (17) is blocked for a certain amount of time (11). This blocking time (11) can be adjusted separately or can comply with its own MAC aging time (12), whereas after

its expiration, entries in the own FDB (13) entries are deleted.

That is, automatically, for a certain amount of time (11), no packet (14) is received by the data plane. Effectively the port (18) is thereby logically blocked. That is, the physical layer stays active, however all incoming packets (14) are abolished. This “logical blocking” also conforms with the blocking of a port (18), as being applied with the so called “Spanning Tree” method.

So for this amount of time (11) no further packets from this port (18) reach into the access network (7). All further network nodes (10) and users (1) respectively are thereby also safe from the attack.

Reference signs

1	Residential Customer / user
2	MAC flooding attack
3	ONT (Optical Network Terminal) / first access node
4	line of demarcation
5	interface to the network user -> port blocked when reaching the limit
6	BRAS / PPPoE termination
7	network
8	aggregation network
9	OLT (Optical Line Termination)
10	upstream network nodes-> also secured
11	blocking time
12	aging time
13	Forwarding database (FDB)
14	packet
15	layer 2 switch
16	MAC address
17	limit (of the maximum quantity)
18	port
19	data plane

CLAIMS

1. A method for protecting a network against a security attack from an user, and in particular, for a layer 2 switch, against a MAC flooding attack, in which

the MAC flooding attack floods the layer 2 switch with at least one packet,

a database is provided which saves a MAC address and its allocation,

the database has a maximum quantity,

characterized in that,

an interface (5) between the user (1) of the network (7) and a network access functions as a line of demarcation (4),

when the limit of the maximum quantity for a port (18) is reached, the port (18) is blocked during a blocking time (11).

2. A method according to claim 1, wherein the limit of the maximum quantity (17) is a limit per configuration.

3. A method according to claim 1, wherein the limit of the maximum quantity (17) is a per default provided limit.

4. A method according to any one of claim 1 to 3, wherein the blocking time (11) is greater than an aging time (12).

5. A method according to any one of claims 1 to 4, wherein the aging time (12) is alterable.

6. A method according to claim 5, wherein the aging time (12) is 200 s.

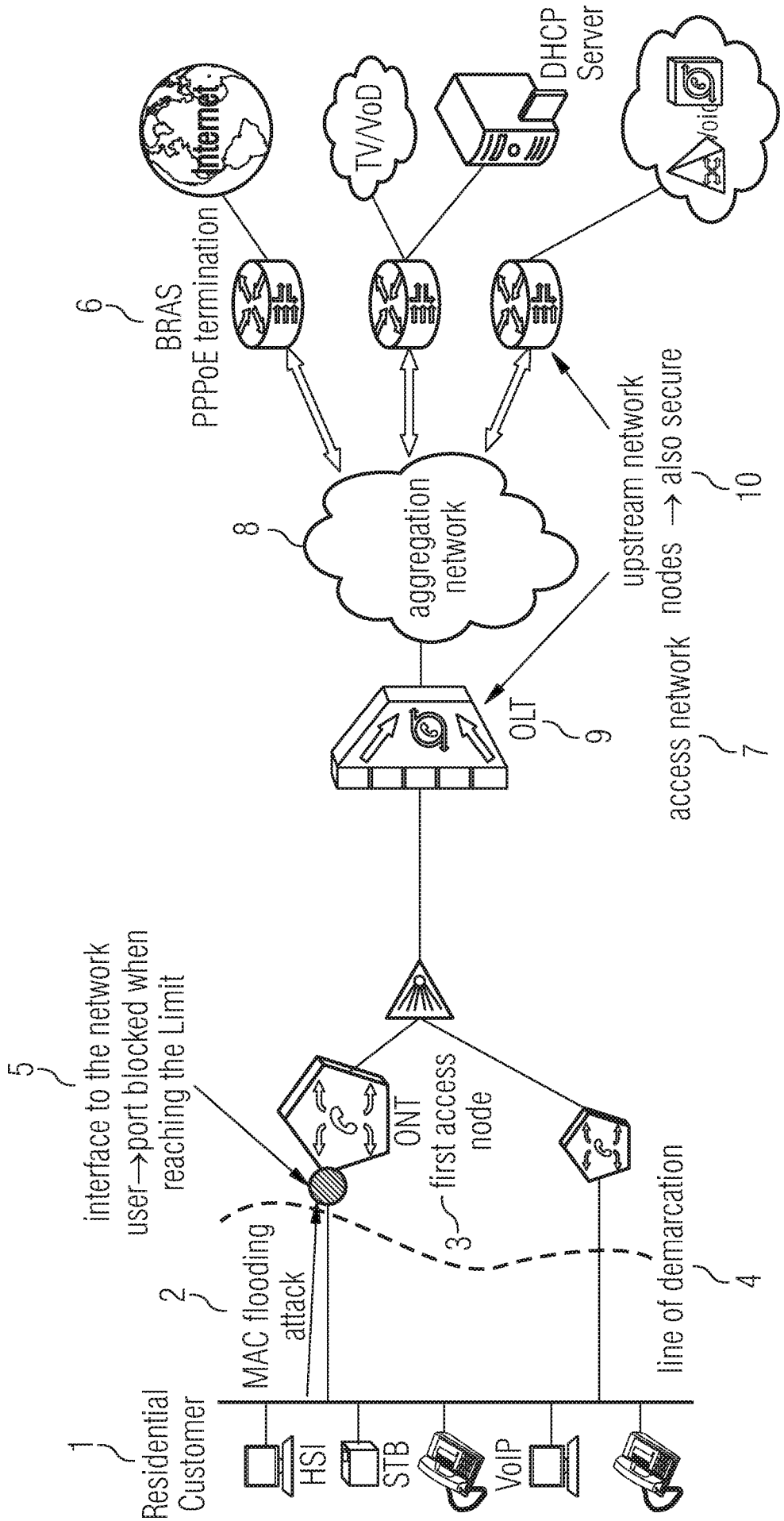
7. A method according to any one of claims 1 to 6, wherein the blocking time (11) can be adjusted separately.

8. A method according to any one of claim 1 to 7, wherein the blocking time (11) can comply with its own aging time (12).

9. A method according to any one of claims 1 to 8, wherein a hysteresis is provided between a blocking and an unblocking of the port (18).

10. A method according to claim 9, wherein two different reasonable limits (17), for the blocking and the unblocking of the port (18) are provided.

11. A method according to any one of claims 1 to 10, wherein the method can be switched off.


Residential Customer
1
HSI
STB
VoIP
MAC flooding attack
2
line of demarcation
4
ONT
first access node
3
interface to the network
user → port blocked when reaching the Limit
5
access network
7
OLT
9
aggregation network
8
upstream network nodes → also secure
10
BRAS
PPPoE termination
6
Internet
TV/VoD
DHCP Server
VoD